

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

YOUR SECRET WEAPON IN THE WAR ON FRAUD

VOLUME 13 NO.12
DECEMBER 2011

IN THE NEWS

If Fraud Occurs, It May Be Your Fault

“Companies are failing to read and to act quickly on the warning signs of fraud.”
Recent findings by KPMG:

- The number of fraud cases preceded by a red flag rose to 56% of all frauds—up from 45% in 2007.

- Instances where action was taken following the initial appearance of a red flag plunged dramatically—from 24% in 2007 to just 6% in 2011.

Critical lesson: Ignored red flags are a license to steal for fraudsters...and a potentially costly lost opportunity for the organization to reduce fraud losses and associated costs.

Also important: According to the Association of Certified Fraud Examiners, the average fraud lasts 18 months. Such long-running frauds often result in numerous red flags. This suggests that organizations often have multiple opportunities to shut down fraudulent activity and minimize their losses. The key is knowing what the red flags are and having processes and procedures in place to report and act on them.

White-Collar Crime Fighter source: “Who Is the Typical Fraudster?”, a global survey by KPMG, www.kpmg.com.

IN THIS ISSUE

- **COUNTER-CORRUPTION**
Bribery and corruption—new traps to avoid 3
- **CYBER-CRIME FIGHTER**
The threats for 2012..... 4
- **IDENTITY DEFENSE**
Preventing organizational identity theft..... 5
- **THE CON'S LATEST PLOY**
Law-enforcement successes from around the country.....7

Paul McCormack, CFE, *Connectics*

Five Facts About Fraud That Companies Learn the Hard Way



Fact #1: Fraud does not happen on the company's timetable. Revenues are up.

Revenues are down. It doesn't matter. The company could be experiencing the best of times, or the worst of times. Fraudsters don't care. All they want is your money.

They decide, if, when, how much and how often to steal. If the organization has countermeasures in place, the fraud may be prevented, or the losses kept to a minimum.

What to do: Be proactive. It is never too early to develop countermeasures. Begin by conducting an assessment of how well your company is positioned to detect, prevent and investigate fraud today. Then, document what the optimal fraud program looks like. The difference between where your organization is today and where it should be can then be broken down into discrete steps or projects.

Key: You can't pick when fraud will take place. You can control what your organization is doing to fight fraud.

Fact #2: Fraud scares people, especially senior executives. When I meet with clients I often tell them that fraud is a small word with big implications. In my experience, senior executives are often apathetic about fraud. That is, until they are made aware of an actual fraud taking place on their watch. Then they become exceptionally nervous and spend a great deal of energy worrying about what will happen. They don't know what they don't know and that makes them more nervous. Is this my fault? Will I be

blamed? How much money will we lose? Will we get it back?

What to do: Educating senior executives on the basics of fraud as well as how the company is positioned to combat theft can help put things in perspective. With the benefit of fraud awareness training, senior leadership may overreact to

The company could be experiencing the best of times, or the worst of times. Fraudsters don't care. All they want is your money.

news of wrongdoing. This can result in uninformed decisions that exacerbate the problem.

Key: Balance the need to communicate fraud risks and actions intended to address incidents of fraud against making it appear that the “sky is falling.”

For auditors, security managers and others involved: During any briefing session with senior leadership, don't share a problem without a solution. If an executive is made aware that fraud losses are increasing, be prepared to explain tactics that can help reduce or hold losses at current levels. Also be prepared to ask for additional resources to develop the organization's anti-fraud function. The best time to ask for such resources is when senior executives are made aware of potential gaps, or actual incidents of fraud.

Fact #3: Fraud prevention is an afterthought in most companies. It shouldn't be, but it is. Most organizations don't think about fraud until it happens, or they narrowly avoid taking a loss. There is no reason that organizations need to experience the vast majority of employee and third-party fraud. You can never be “fraud free,” but it certainly is possible to make it much more difficult for wrongdoing.

ers to commit most schemes.

What to do: Have an independent anti-fraud professional report a senior executive's answers to the following key questions:

- Do you have an employee fraud hotline? How do you measure its effectiveness?
- Do you have a fraud case management database? If so, when was the last time the information was used to develop proactive countermeasures?
- What controls do you have in place to prevent and detect fraud? Who "owns" control development, deployment and testing?
- What policies and procedures do you have in place to ensure that employees are unable to steal your company's intellectual property? When was the last time someone tested their effectiveness?
- How often does fraud take place in your industry?
- Have you incorporated "lessons learned" from frauds that occurred at other companies?

You can never be "fraud free," but it certainly is possible to make it much more difficult for wrongdoers to commit most schemes.

• Who is responsible for fraud prevention, detection and investigation within your organization? If separate departments are involved, how often do they meet to share intelligence?

Key: Very rarely will senior executives answer these questions without mentioning areas for improvement. Most often, they struggle to answer at least one or two of the questions which can lead to some uncomfortable silences and pained expressions. However, the exercise helps them to identify what is needed to prevent fraud, and can potentially provide at least a partial roadmap for getting there.

Fact #4: Fraud investigations are easy to "screw up." Investigating fraud, particularly employee fraud, is much more complicated than it appears. If in the course of an investigation an employer violates any of the numerous rights that employees have, the "hunter" can quickly become the "hunted." *Example:*

Local law enforcement thinks that one of your employees, Bob, is involved in drug trafficking. Your internal audit department is also investigating Bob. They plan to talk with him next week regarding some missing inventory.

A detective from local law enforcement wants internal audit to ask a couple of questions that would help him with the drug investigation. In fact, the detective really wants to be in the room during the meeting. Helping law enforcement is a good idea, right? We might need them to help "go after" Bob for the inventory we think he has stolen. Would we "screw up" the investigation by helping law enforcement? How? We've already sent an email to the detective detailing the inventory theft. The detective agrees—this guy is a criminal!

What to do: Ideally, there should be at least one experienced fraud investigator on the team with the appropriate fraud experience and qualifications. Gathering information for law enforcement at their direction to aid in criminal prosecution of an employee can violate the employee's legal rights.

Never proceed without notifying legal counsel—be it an attorney with the company, or a lawyer with an outside firm that your organization has engaged. An experienced employment lawyer can easily make the difference between a successful investigation and a disaster that costs the investigator his job and leaves the alleged fraudster in

"Detecting, Preventing and Auditing Fraud Using Data Analysis"

Earn CPE Credits Without Leaving Your Computer!

A NEW 2012 "HOW-TO" LEARNING SERIES FROM AUDITNET AND FRAUDAWARE

Get Expert Advice on how to stay a step ahead of fraudsters with proven tactics and techniques.

After completing this carefully designed series of 18 high-impact Webinars featuring the anti-fraud profession's top experts, your auditors, investigators, accounting staff, financial personnel, compliance officers and senior management teams will have a unique body of knowledge, skills and abilities to launch highly effective initiatives that beat fraudsters at their own games—affordably and efficiently.

Sign up now for this unique series of learning sessions that gets right to the brass tacks of using your organization's resources to safeguard its financial, intellectual and physical assets from the growing army of fraudsters.

For full details, dates, CPE credits and registration options, **PLUS VALUABLE FREE BONUSES** please visit <http://www.auditnet.org/2012Webinars.htm>

WHITE-COLLAR CRIME FIGHTER

Editor

Peter Goldmann, MSc, CFE

Consulting Editor

Jane Y. Kusic

Managing Editor

Juliann Lutinski

Senior Contributing Editor

David Simpson

Associate Editor

Barbara Wohler

Design & Art Direction

Ray Holland, Holland Design & Publishing

Panel of Advisers

Credit Card Fraud

Tom Mahoney, Merchant 911.org

Forensic Accounting

Stephen A. Pedneault, Forensic Accounting Services, LLC

Fraud and Cyber-Law

Patricia S. Eyres, Esq., Litigation Management & Training Services Inc.

Corporate Fraud Investigation

R.A. (Andy) Wilson, Wilson & Turner Incorporated

Corporate Integrity and Compliance

Martin Biegelman, Microsoft Corporation

Securities Fraud

G.W. "Bill" McDonald, Investment and Financial Fraud Consultant

Prosecution

Phil Parrott, Deputy District Attorney Denver District Attorney's Office, Economic Crime Unit

Computer and Internet Investigation

Donald Allison, Senior Consultant, Stroz Friedberg LLC

Fraud Auditing

Tommie W. Singleton, PhD University of Alabama at Birmingham

White-Collar Crime Fighter (ISSN 1523-0821) is published monthly by White-Collar Crime 101, LLC, 2417 Havershire Dr., Raleigh, NC 27613. www.wccfighter.com. Subscription cost: \$295/yr. Canada, \$345. Copyright © 2011 by White Collar Crime 101, LLC. No part may be reproduced without express permission of the publisher.

Mission Statement

White-Collar Crime Fighter provides information of maximum practical value to organizations and individuals involved in all facets of investigating, detecting and preventing economic crime.

This community includes law internal auditors...fraud examiners...regulatory officials...corporate security professionals...senior executives...private investigators...and many more.

The editors of *White-Collar Crime Fighter* strive to gather and compile the most useful and timely information on economic crime issues.

Comments, suggestions and questions are welcome. Please fax us at 203-431-6054, or E-mail us at editor@wccfighter.com. Visit us on the Internet at www.wccfighter.com.

place and unpunished.

Fact #5: Fraud losses are rarely recovered. We'd like to think that law enforcement can reach out and claw back the proceeds from a fraud whenever needed. The truth is that most of the time, the proceeds are long gone. Fraud schemes last a median of 18 months. During that time, your organization's money is burning a hole in the pocket of the fraudster. They want to buy goods, services, pay down debt, stop foreclosure, share their good fortune with family and friends etc. They typically don't deposit the money in their bank account and watch it earn interest.

Making matters worse, law enforcement is often unable or unwilling to

Avoid adopting the view that law enforcement or the civil litigation community will recover fraud proceeds.

help organizations recover fraud losses. Law enforcement is thinly stretched. At the local level, detectives in small cities are assigned cases from petty theft to murder. In larger jurisdictions, detectives have an overwhelming case backlog that is closely tracked by their superiors. Financial crimes can be extremely complicated and time consuming to investigate, especially if the detective does not have a financial background. Detectives need to close cases—quickly.

At the federal level, the bar is even higher. A six-figure loss may be devastating for your organization, but it may barely raise the eyebrow of an FBI agent in a large city. With no connection to organized crime, drugs or terrorism, the case file may be shelved and forgotten.

What to do: Avoid adopting the view that law enforcement or the civil litigation community will recover fraud proceeds. Even if entirely successful, any amounts recovered will be reduced by professional fees paid to attorneys, forensic accountants, etc. And, if you don't engage a private third-party asset recovery firm, you risk having employees spend countless hours documenting the fraud which will ultimately mean other tasks are neglected that may actually open the door for additional fraud.

White-Collar Crime Fighter source:

Paul McCormack, CFE, co-founder and Executive Vice President of Connectics, an Atlanta, GA-based consulting firm. Paul is also former vice president of fraud detection for SunTrust Banks in Georgia. He can be reached at pmccormack@innovarpartners.com.

COUNTER-CORRUPTION

Brian P. Loughman and Richard A. Sibery,
partners, *Ernst & Young LLP*

Bribery and Corruption: New Traps to Avoid



The legal dangers have never been greater for companies seeking to expand their operations overseas. The Foreign Corrupt Practices Act (FCPA) and the newly enacted UK Bribery Act together represent a formidable compliance framework, violators of which pay a devastating fee.

Most notable example: Siemens AG, the German-based multinational manufacturer of diversified products, paid nearly \$13 million in suspicious payments to foreign entities between 2001 and 2007, including \$4.5 million in bribes to Nigerian government officials to secure four lucrative telecommunications products for Nigerian state-owned entities. The company ended up paying \$1.6 billion in penalties to the US and German governments.

Whether Siemens's executive team condoned this activity is unknown. What is clear is that many companies get into trouble when overseas managers pay bribes without awareness of the potential penalties.

The message could not be clearer—formulate and rigorously enforce a strict compliance policy, including detailed procedures for doing business abroad.

Among the most crucial components of such a policy is thorough due diligence.

Details: The FCPA places responsibility on companies that are considering acquisition of a foreign entity to conduct comprehensive due-diligence procedures on the overseas target company(ies).

Moreover, the acquiring company may be held liable for any corrupt activity that occurred before the acquisition took place—even if it had no direct knowledge of the activity.

DUE SELF-DEFENSE

The single most critical function for

minimizing the risk of corruption in an acquisition or business contract with an overseas entity is thorough due diligence.

Step 1: Put together a qualified due diligence team. The team conducting due diligence at the pre-transaction stage should comprise attorneys and forensic accountants.

Important: The anti-corruption due diligence procedure should be conducted simultaneously with “regular” financial due diligence procedures—to reduce duplication of information that must be obtained from the target organization.

Step 2: Corruption risk assessment. This step may be part of an overall risk assessment of the proposed overseas venture. However, it should also encompass gathering an understanding of the target organization's operations—including understanding the industry and the countries in which the organization operates.

Key: Ensure that this analysis focuses not just on the physical location(s) of the business but also the countries where its customers are located.

Reason: Some industries are believed to be especially corrupt simply because of an unusually “cozy” relationship that they have with ranking government officials. *Examples:*

- Defense
- Energy
- Financial services

Essential: The due diligence team should apply extra scrutiny to target companies from high-risk industries located in high-risk countries. They can streamline their work by focusing on transactions most likely to be exploited

Cyber-Crime Outlook:

Threats to Prepare for in 2012...and Beyond

For Sony, RSA and untold numbers of additional organizations sabotaged or defrauded by cyber-criminals, 2011 was one of the most unusual years in the history of IT security. So what does 2012 have in store for us?

We asked our Websense Security Labs for their 2012 predictions.

Result: *Our list of the probable top cyber-crime events in 2012:*

1. Your social media identity may prove more valuable to cybercriminals than your credit cards. Bad guys will actively buy

and sell social media credentials in online forums. Spammers have been buying and selling large parcels of E-mail credentials for several years now. We've seen carder sites where criminals can buy and sell your credit card information for pennies on the dollar. Want a South African issued card with a \$25,000 limit with the user's PIN? How about one from the U.S. issued by a bank in the Northeast along with the user's Social Security number?

That's old news. Facebook has more than 800 million active users, and over half of them log on daily and they have an average of 130 friends. Trust is the basis of social networking, so if a bad guy compromises your social media log-ins, there is a good chance they can manipulate your friends. Which leads us to prediction #2.

2. The primary blended attack method used in the most advanced attacks will be to go through your social media "friends," mobile devices and through the cloud. Blended attacks used to be predominantly about the use of E-mail and Web together. Many of the recent so-called advanced persistent threats (APTs) were spear-phishing E-mail scams.

Latest threat: In 2012, advanced attacks will increasingly use at least two, and sometimes all, of the following emerging technologies: Social media, cloud platforms and mobile. We've already seen one APT attack that used the chat functionality of a compromised social network account to get to the right user.


3. 1,000+ different mobile device attacks coming to a smartphone or tablet near you. Expect more increases in exposed vulnerabilities from black hats and white hats in the coming months for mobile devices. In 2012, we estimate more than 1,000 different variants of exploits, malicious applications and botnets infecting that device held in your hand and plugged into your head.

Also likely: New versions of malware that access consumer banking and social credentials as well as other sensitive data on mobile phones. This includes work documents and any cloud applications individuals may have on that handy device. We'll also start seeing significantly more social engineering designed to specifically lure mobile users to infected apps and Web sites.

4. Containment is the new prevention. For years, security defenses have focused on keeping cybercrime and malware out. There's been much less attention on watching outbound traffic for data theft and evasive command and control communications. But multiple studies show that the majority of data theft is related to hacking and malware.

In 2012, organizations will look to stop data theft at corporate gateways that detect custom encryption, geolocations for web destinations, and command and control communications. More organizations will implement outbound inspection and will focus on adapting prevention technologies to bolster containment.

5. Scareware tactics and the use of rogue anti-virus, which decreased a bit in 2011, will stage a comeback.

Prediction: Three areas will emerge as growing scareware subcategories in 2012: Fake registry clean-up, fake speed improvement software and fake back-up software mimicking popular personal cloud backup systems. 

White-Collar Crime Fighter source:

Patrik Runald, senior manager of security research, Websense, and "Security Predictions for 2012 from Websense® Security Labs." Websense is a San Diego, CA-based provider of web security, E-mail security and data loss prevention (DLP) services, www.websense.com.

for fraudulent purposes, such as travel and entertainment, gift-giving, charitable contributions and concessions.

Step 3: Analyze target companies' anti-corruption policies/procedures. Lack of such policies and procedures—or of a compliance program in general—is often reason enough to walk away from a prospective overseas deal.

However, if there are formal policies and procedures, be sure to evaluate their stringency and effectiveness. Look at the target's whistleblower hotline as well as the target's structure in the context of anti-corruption compliance.

Step 4: Conduct public searches of target company's foreign subsidiaries and third-party intermediaries. Conduct background searches on the company, its executives and subsidiaries as well as all third-party intermediaries.

Important: Any negative findings about the target company or anyone who works for it should be given special consideration in the final risk evaluation of the company. **Example:** Situations where the target company or subsidiaries cannot be identified in any public compliance or news databases.

Step 5: Conduct interviews of key target company executives. This exercise should commence once you have obtained a "high-level" understanding of the firm's general operations and locations. Cover such topics as the target's business from state-owned entities...any high-level interactions between the target and government officials...details of the anti-corruption policy, etc.

Essential: Conduct interviews with such high-level titles as CEO, CFO, COO, general counsel, sales executive. **Attempt to gather as much detail from these individuals about...**

Business unit operations
 Business transactions with government officials
 Use of third-party intermediaries
 Culture of gift-giving
 Internal controls over accounts payable...cash transactions...payroll...political and charitable donations...FCPA and other anti-corruption compliance activities.

Step 6: Identify potential "red flags." In most, if not all, corrupt foreign companies, there are clear red flags that anti-corruption laws are being broken.

Examples:

The target company is related to a government official.
 Refusal to certify compliance with

INFORMATION SECURITY

anti-bribery and corruption laws.

- Excessive use of cash in business transactions.

- Lack of transaction transparency.

- Payments are made from out-of-country sources, or payments are made to out-of-country bank accounts.

- Charitable contributions are made to an organization with a known affiliation with a government official, customer or representative.

Step 7: Detailed due diligence procedures. Examples:


- Additional interviews. In previous steps, high-level interviews with key executives were conducted. Now it is time to interview individuals “in the trenches.” Finance managers, office secretaries or clerks are often sources of valuable information about potential or actual corruption.

- Transaction record analysis. After identifying areas of high risk—such as third-party intermediaries, commission payments, etc.—your team should conduct forensic accounting procedures to detect wrongdoing or potential FCPA violations. Records to be analyzed may include vendor files ...records of business transactions with government agencies...records of arrangements with customs, tax or regulatory authorities...receipts for travel, gift and entertainment expenses...records of charitable contribution.

Step 8: Ensure that all red flags are satisfactorily resolved. If the target company is not corrupt, there should be legitimate explanations for all red flags. If they cannot be resolved, management must carefully deliberate the prudence of moving forward with the deal.

Step 9: Enforce compliance after the closing. The fact that your pre-closing due diligence has resulted in a green light for the transaction does not mean that bribery or corruption problems won't arise down the road.

Solution: Ensure that a senior officer is responsible for oversight of bribery and corruption monitoring. Reinforce anti-bribery and corruption policies on a regular basis, including policies governing travel and entertainment expense, gift-giving and charitable giving.

Also important: Anti-corruption training. All employees should receive training customized to the business operations in which they work, such as finance, accounts payable, operations, etc. 

White-Collar Crime Fighter sources:

Brian P. Loughman, partner, Ernst & Young LLP and Americas Leader of the Fraud Investigation & Dispute Services Practice and Richard A. Sibery, partner, Ernst & Young LLP and head of the Fraud & Investigations Group. Loughman and Sibery are coauthors of *Bribery and Corruption. Navigating the Global Risks*, John Wiley & Sons, www.wiley.com.

Eleanor E. Spring, CFE, CRT,
Spring Action Fraud Elimination

What Management Needs to Know to Prevent Organizational Identity Theft



When we think of identity theft we tend to think about an individual's personal information being stolen. But, what about theft of an organization's trade secrets...or the hijacking of a Web site...or customer and employee data breaches?

These are all forms of identity theft or fraud committed against organizations. And they can be extremely damaging.

Key: The target of a fraud may be an individual within your organization or the organization itself. Criminals use a wide range of methods and approaches to commit their crimes. Their aim is usually to steal sufficient information to assume the identity of the person or the business with the goal of fraudulently obtaining goods, services or credit.

Examples:

- **Heartland Payment Systems, 7-Eleven and Hannaford Brothers.** Federal authorities indicted three men in New Jersey in a massive identity theft scheme. “Mr. X” of Miami was charged with acting with two unnamed co-conspirators to locate large corporations and steal vital account information in a crime that the Department of Justice called “the single largest hacking and identity theft case ever prosecuted.”

More than 130 million credit and debit card numbers were stolen in a data breach involving three corporations. The card numbers, along with additional account information, were stolen from Princeton-based Heartland Payment Systems; 7-Eleven Inc., a Texas-based convenience store chain,

and Hannaford Brothers Company, a Maine-based super-market chain.

According to the Justice Department, the suspects used a sophisticated hacking technique called an “SQL injection attack,” which “seeks to exploit computer networks by finding a way around the network’s firewall to steal credit card and debit information.”

- **Study by CPP Group**—an identity theft prevention service provider—shows 100,000 small and medium enterprises (SMEs) falling victim to ID fraud. The UK-based research shows that identity thieves are now “trading up” from personal to corporate fraud as they clone the identities of entire businesses. It was found that one in five SMEs admit they may be vulnerable to corporate identity theft due to lax information security procedures and protocols, but, according to the study, “this figure could soar as criminals catch on to a loophole with Companies House data processing.” (Companies House is the agency responsible for registering and storing information on UK-based corporations.)

Criminals use a wide range of methods and approaches to commit their crimes.

According to the study, “this figure could soar as criminals catch on to a loophole with Companies House data processing.” (Companies House is the agency responsible for registering and storing information on UK-based corporations.)

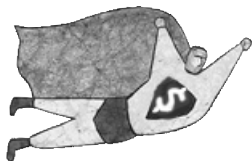
DEADLY COMBINATION

Corporate identity theft is composed of a deadly combination: A world full of unsecured wireless activity and computers operated by criminals in ways that enable seemingly easy illegal access to sensitive data. In fact, hacking into company systems and databases appears to have become a favorite identity theft technique because it is so easy to carry out.

PROTECT YOUR ORGANIZATION

Depending on your type of business, there are three main anti-identi-

FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE



Fraud's Friend...Management Complacency

Fraud is an ever-evolving threat that has embraced technology for new implementations and for the ability to change its forms. This has enabled fraud to attack new weak points and to hide until new detection methods are developed. It has also greatly shortened the amount of time necessary to commit fraud—as transactions are now completed at the speed of the Internet.

Key: The fraudsters are better prepared, better hidden and have much less exposure time during the commission of a fraud.

Problem: Management complacency. The “set it, forget it” mindset is pervasive among organizations. It involves putting safeguards into place and then going back to business as usual. Fraudsters make a living seeking out control weaknesses, so as soon as a preventive measure becomes obsolete, new opportunities to victimize organizations emerge.

Essential: Ongoing vigilance...in a continuous, concerted way. This should include software updates, staff training, activity monitoring, customer education and continuous screening for operational weaknesses.

White-Collar Crime Fighter source: Dean Goodlett, assistant vice president and fraud investigations manager in the financial intelligence unit of Rabobank, quoted in *Fraud and Financial Crime*, Special Report sponsored by DeticaNetReveal, an enterprise risk, fraud and compliance solution for detecting and managing fraud, risk and crime. <https://www.deticanetreveal.com/en/>.

Updated SANS Training for Latest Cyber-Threats

Over the past two years, all organizations have seen a dramatic increase in sophisticated attacks against organizations. Cyber-attacks originating from China named the Advanced Persistent Threat (APT) have proved difficult to suppress. Financial attacks from Eastern Europe and Russia obtain credit card, and financial data are also resulting in millions of dollars stolen.

Commercial and Federal IT security experts have been battling multiple intrusions attributed to the APT during the past several years with varying degrees of success. Management may want to consider providing the latest cyber-forensic training to its senior IT and/or information security staff.

Helpful: Over the past two years, the leading information security training provider, SANS has been updating its forensic and incident response training courses to include the latest tactics needed for finding and defeating the APT. **Examples:**

- **Finding malware in the dark.** Digital forensic investigators are often handed a hard drive and asked to “Find Evil”—though they don’t know where to start looking. In SANS’s training, there is a new section that deals solely with examining compromised systems looking for unknown malware. This process utilizes many of the skills to simply “find evil” when you don’t know where to look.

- **Timeline analysis and super-timeline analysis.** The past two years has seen the dramatic increase in the necessity of timeline analysis for incident response and digital forensics. Forensic experts can now learn to automatically track system activity at a glance. Through examining file system, Windows OS artifacts, and registry entries from a single machine, an examiner can determine exactly what happened at any time.

- **Enterprise investigations.** Investigators must utilize new techniques to not only investigate a single system, but hundreds simultaneously.

Solution: “F-Response Tactical”—which enables investigators to remotely examine a system without first having to image it. This increase in efficiency is needed to quickly scan systems during a large-scale breach.

Full details: FOR508:Advanced Computer Forensic Analysis and Incident Response <<http://computer-forensics.sans.org/courses/description/advanced-computer-forensic-analysis-incident-response-98>> at <http://computer-forensics.sans.org/courses/description/advanced-computer-forensic-analysis-incident-response-98>.

White-Collar Crime Fighter source: SANS Computer Forensics and Incident Response, <http://computer-forensics.sans.org/>.

ty theft essentials...

- **Safeguarding the organization's sensitive business information.** This includes product or service trade secrets, proprietary marketing strategies and financial data.

- **Protecting customer and employee information.** Known as Personal Identifying Information—or PII—this includes Social Security numbers, dates of birth, addresses and credit card data.

- **Complying with information security laws.** Every business, be it large or small, must deal with state and federal workplace information protection and privacy rules and every precaution should be taken to protect the PII of all employees and clients.

HOW TO GET THERE

- **Enhance the security on all computers and networks.** One of the most common methods of stealing an organization’s identity is through IT systems.

Phishing Web sites which use keystroke logging software to record keyboard strokes are another way identity thieves steal financial details.

Self-defense: Limit employee access to the Internet. Not every employee is required to have Internet access to fulfill their job requirements. Employees browsing the Web could inadvertently download so-called spybots and viruses which could expose your sensitive data to theft.

- **Safeguard on-line financial transactions.** If your organization does on-line banking and bill paying, consider setting up a separate workstation that only authorized personnel can make use of. This workstation should never be used for general Web browsing or emailing. Install routers and firewalls to prevent unauthorized access. Keep your anti-virus and anti-spyware software up to date. Talk to your IT staff to make sure your default settings give you as much security as possible.

- **Put the Federal Trade Commission's so-called Red Flags Rule into effect.** This set of federal anti-identity theft rules requires many organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs—or “red flags”—of identity theft in their day-to-day operations. (For details, visit <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.) They should be enforced with written compli-

ance policies and be reviewed at least once a year for any new information which should be included.

- **Educate employees regarding protocol in responding to threats of identity theft.** Uneducated employees will always be the weakest link and all the controls in the world won't change that. If employees don't know how to identify and deal with threats to their own or their employer's identity, it is only a matter of time before one of them discloses information that results in identity theft.

If your organization does online banking and bill paying, consider setting up a separate workstation that only authorized personnel can make use of.

- **Consider hiring a Chief Identity Theft Prevention Officer.** Companies concerned with increasing identity theft risks should consider appointing or hiring a Chief Identity Theft Prevention Officer (CITPO) to design, implement and monitor the organization's efforts for reducing identity theft risks.

- **Put policies and procedures in place which involve interrogating internal systems** to detect soft spots that may be vulnerable to identity theft.

- **Use a cross shredder.** A highly effective information security measure is to have management shred all sensitive information themselves rather than putting sensitive documents into the unknown hands of an outside shredding company.

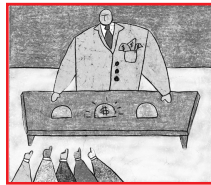
- **Destroy computer and copier hard drives before discarding them.**

- **Conduct rigorous background checks to validate all new hires' identities** and confirm completeness and accuracy of employment by performing thorough background checks.

In addition, as more and more confidential information is stored on employees' mobile storage devices, management should seek new ways to protect that data through policies and automated tools for detecting and preventing unauthorized usage and storage. 📄

White-Collar Crime Fighter source:

Eleanor E. Spring, CFE, CRT, fraud investigator at Spring Action Fraud Elimination, www.springactionfraud.com. Eleanor is a REID Certified Interrogator (CRT). She can be reached at eleanor@springactionfraud.com.



THE CON'S LATEST PLOY...

From *White-Collar Crime Fighter's* files of new scam, scheme and scandal reports

Madison, WI

“Bad judgment” drove octogenarian executive to orchestrate bank/insurance fraud scheme. David R. Scholfield, 84, the former CEO of Manson Insurance, was accused of forging customer signatures on loans to finance phony insurance premiums, embezzling credits from insurance companies and fraudulently billing customers.

Scholfield admitted that he used “bad judgment” in his business practices and was apologetic to Judge William Conley during Scholfield's sentencing hearing in U.S. District Court in Madison, WI.

Details: According to the indictment, Scholfield had one of his employees forge customers' signatures on insurance premium financing notes that his agency made available for facilitating the purchase of insurance policies. After the signatures were forged, Scholfield and another co-conspirator employee signed the notes as officers of Manson. They then signed the backs of the notes—indicating that the notes were being sold by Manson to River Valley Bank with their personal guarantees.

River Valley Bank paid the face value of the notes to Manson which collectively resulted in a \$1.9 million loss.

Scholfield was sentenced to five years in prison.

Columbus, OH

Stealing millions and pleading guilty to tax fraud. Shaun Allen Clark pleaded guilty to charges in connection with a \$2.3 million embezzlement scheme. He faces a maximum prison sentence of 10 years and a fine of up to \$250,000.

Clark pleaded guilty to one count of willfully filing a fraudulent federal

income tax return with Internal Revenue Service (IRS) and to two counts of money laundering.

Background: According to court documents, in January and February of 2008 Clark embezzled two checks totaling \$24,450 from his employer, The Scotts Company of Marysville, OH. Shortly thereafter, Clark began working as the Controller for US Bridge, a 70-year-old metal bridge construction firm located in Cambridge, OH. Between April 2008 and September 2009, Clark embezzled approximately \$2,310,006 from US Bridge.

Clark was authorized by US Bridge management to initiate wire transfers via the Internet from US Bridge bank accounts in order to remotely transfer funds to a payroll company and suppliers of steel and other raw materials. Clark used this remote access to US Bridge bank accounts to transfer funds into his own personal bank accounts.

As Controller, Clark was responsible for all bookkeeping and accounting work involving US Bridge and its subsidiary companies. Clark entered false entries into the journals and ledgers of US Bridge and its subsidiaries in order to conceal his embezzlement activities. In turn, the false journal entries were used to generate fraudulent financial statements for the company.

Problem: Clark was the primary point of contact for US Bridge regarding a line of credit the company maintained with the company's bank. Clark submitted the false financial statements to the bank for the purpose of conforming with the bank's financial performance requirements and thereby maintaining the line of credit.

Maintaining the line of credit of course helped to conceal Clark's illegal activities and to further fund his

embezzlement scheme.

Productive use of stolen funds: On or about December 23, 2008, Clark wrote a check from his personal bank account—now flush with embezzled cash—to the Ohio State University (OSU) in the amount of \$100,000 in order to secure Buckeye Club season tickets to OSU football games.

Details: To pay for the tickets—and other high-end items—Clark embezzled a total of \$996,982 from The Scotts Company and US Bridge during 2008.

Unsurprisingly, Clark omitted this income from his 2008 federal income tax return; thus, resulting in a tax loss to the IRS of \$336,028.

During the investigation, the IRS seized \$101,788.35 from various financial accounts controlled by Clark, as well as a Chevy Tahoe truck and a boat purchased by Clark with proceeds of the embezzlement. The proceeds from the forfeitures of these assets were returned to US Bridge.

Clark was released on bond. A sentencing date has yet to be set.

Newark, NJ

Mini-Madoff scheme results in \$80 million in losses and loss of one innocent life. Charles K. Schwartz, the founder of Allied Health Care Services, Inc., a New Jersey-based company supposedly dealing in

durable medical equipment, pleaded guilty to a \$135 million financial fraud scheme.

Details: Schwartz arranged with an unindicted co-conspirator who owned a company identified by the FBI simply as Company 1 to have phony invoices for medical equipment sent to Allied. The invoices supposedly indicated that Company 1 had leased the equipment to Allied which in turn wished to finance the leases through bank financing. Allied therefore forwarded the invoices to various financial institutions for the purposes of securing such financing.

In several cases, the ploy succeeded.

Examples:

- In one case, a financial institution provided \$250,000 directly to Company 1 on the strength of a phony invoice for that amount from Allied.

- A similar incident involved the disbursement to Company 1 of a \$2 million check for medical equipment purportedly provided by Company 1 to Allied, but in fact not provided at all.

In all cases, Company 1's owner would keep 3% to 5% of the "proceeds" from the financial institutions and forward the balance on to Charles Schwartz or companies owned by him.

To make the payments on leases provided by the financial institutions, Schwartz perpetuated the scheme with similar "deals," thereby using fraudulently obtained cash from banks to cover payments on earlier-concluded

leases. The scheme thus resembled the Ponzi scheme run by Bernard Madoff with the exception that Madoff's victims were primarily individuals whereas Schwartz's were banks.

Schwartz reportedly used the approximately \$80 million to purchase land in upstate New York, a large home in New Jersey and other high-priced properties.

Another tragic Madoff similarity: An unidentified employee of one of the defrauded banks in the Schwartz fraud committed suicide in the aftermath of the incident. According to the US Attorney, "Despite the fact that he had nothing to do with the fraud here, he felt that his reputation would be forever damaged in a way that nobody would ever trust him in the future."

The suicide is eerily reminiscent of the suicide by Madoff's son, Mark in December 2010.

"Detecting, Preventing and Auditing Fraud"

Earn CPE Credits AND GET A FREE KINDLE!!!

TWO SPECIAL NEW "HOW-TO" LEARNING SERIES FOR 2012 FROM AUDITNET AND FRAUDWARE

Sign up now for these unique series of learning sessions that get right to the brass tacks of using your organization's resources to safeguard its financial, intellectual and physical assets from the growing army of fraudsters.

For full details, dates, CPE credits and registration options, **PLUS VALUABLE FREE BONUSES** please visit <http://www.auditnet.org/2012Webinars.btm>

COMING SOON IN

White-Collar Crime Fighter...

- Overcoming fear of using audit software to detect fraud
- Using the psychology of fraudsters to catch them
- Information security strategies for non-technical decision-makers
- Locating hidden assets in fraud cases



YES... I want to save \$100 on a one-year subscription to *WHITE-COLLAR CRIME FIGHTER!* By subscribing now, I'll get the money-saving introductory subscription rate of \$150. **That's \$100 off the regular subscription price of \$250!**

Plus, send me—for **FREE**—The new book, *Detecting and Preventing Fraud in Accounts Payable*. This is a \$50 value—yours absolutely **FREE** with your subscription to *White-Collar Crime Fighter!*

Payment enclosed (or) Charge my Visa Mastercard AMEX Discover Bill me

Card # _____ Expiration date _____

Signature _____

Name _____

Affiliation _____

Address _____

City _____ State _____ Zip _____

Call 1-800-440-2261...Or Fax this order form to: 203-431-6054

Or subscribe on-line at www.wccfighter.com.

Or mail this form and your check to: White-Collar Crime Fighter, 213 Ramapoo Rd., Ridgefield, CT 06877. You can contact White-Collar Crime Fighter by E-Mail: subscribe@wccfighter.com